Institution		**Date of Exam**	
Charter		**Prepared By**	

11- INFORMATION TECHNOLOGY RMP
SNAPSHOT WORKPROGRAM

INSTRUCTIONS

1. **Review the IT Officer's Questionnaire (ITOQ) and comment on any responses from the ITOQ that result in a finding.**

2. **Provide responses to the general questions at the end of each PART in the boxes labeled "Examiner Comments" or "Additional Comments".**

3. **Complete the Summary of Findings at the end of the workprogram.**

If this is a Streamlined/ Level II Exam:

1. **Document a response to any questions from the IT Officer's Questionnaire that results in a finding.**

2. **Perform only Parts 1 (Risk Assessment), 3 (Audit), 4 (Disaster Recovery), and 6 (GLBA) of the IT RMP and the other sections at the discretion of the EIC. This is consistent with FDIC instructions. The questions under Part 2 (Operations), and 5 (Vendor Management) will be answered "DNP" or did not perform. These questions will be answered under the discretion of the EIC or when there is a "no" answer in the questionnaire that needs to be explained.**

   The #5 - wire transfer procedure, #16 - UIGEA, #14 - ID Theft Red Flags, and #15 - Remote Deposit capture should be performed. #14 and #16 may be waived if they have already been reviewed at a previous exam. #15 may be waived if the institution does not perform RDC activities.

3. **For not report worthy findings, use "list left with management" to streamline the completion of the Summary of Findings page.**

Institution		**Date of Exam**	
Charter		**Prepared By**	

11- INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 1 – RISK ASSESSMENT

An IT risk assessment is a multi-step process of identifying and quantifying threats to information assets in an effort to determine cost effective risk management solutions. Assess the risk management practices and the actions taken as a result of the risk assessment.

1. Evaluate and comment upon whether the risk management process provides a comprehensive program to identify and monitor risk relative to size, complexity, and risk profile of the entity.

Examiner Comments:

2. Evaluate and comment upon whether management and the Board have demonstrated the ability to successfully address existing IT problems and potential risks, including prompt resolution of audit and regulatory concerns.

Examiner Comments:

If needed, provide additional comments regarding the bank's risk assessment function.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

11- INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 2 – OPERATIONS SECURITY AND RISK MANAGEMENT

A strong security program reduces levels of reputation, operational, legal, and strategic risk by limiting the institution's vulnerability to intrusion attempts and maintaining customer confidence and trust in the institution. Asses how the institution manages and controls risk through the information security program.

1. Evaluate and comment upon the degree to which the organization provides technology services that are reliable and consistent.

Examiner Comments:

2. Evaluate and comment upon whether written technology plans, policies, procedures, and standards are thorough and properly reflect the complexity of the IT environment. Also, evaluate and comment upon whether these plans, policies, procedures and standards have been formally adopted, communicated, and enforced throughout the organization, including a formal written data security policy and awareness program.

Examiner Comments:

3. Evaluate and comment upon whether logical and physical security for all IT platforms is closely monitored, and whether security incidents and weaknesses are identified and quickly corrected.

Examiner Comments:

4. Evaluate and comment upon the degree to which IT operations are reliable, and risk exposure is successfully identified and controlled. Include in this evaluation criteria, an assessment of management's risk mitigation in the payment systems area (including wire transfer and ACH activities).

   For Trust companies:
   a. Review the user list of the TC's cash management system. Review all accounts/systems.
   b. Is dual control required by policy and/or system setting?
   c. What access and abilities does the "administrator" have?
   d. What controls are in place to change user settings like:
      i. Email address for users and administrators

ii. Add/Delete users?

e. Review the employee awareness program and additional controls in place that are used to prevent corporate account takeover (CATO) incidents.

Examiner Comments:

5. Evaluate and comment upon the degree to which IT strategic plans are well-defined and fully integrated throughout the organization.

Examiner Comments:

6. Evaluate and comment on whether management and the Board routinely demonstrate the ability to identify and implement appropriate IT solutions while effectively managing risk.

Examiner Comments:

7. Evaluate and comment upon whether project management techniques and the Systems Development Life Cycle (SDLC) are fully effective and supported by written policies, procedures, and project controls that consistently result in timely and efficient project completion.

Examiner Comments:

8. Evaluate and comment upon the degree to which an independent quality assurance function provides strong controls over testing and program change management.

Examiner Comments:

9. Evaluate and comment upon whether technology solutions consistently meet end-user needs.

Examiner Comments:

10. Banks should be aware of the risks posed by the potential disclosure of sensitive customer information stored on the hard drive or flash memory of photocopiers, fax machines and printers used by the institution. Determine if the bank has written policies and procedures to identify devices that store digital images of business documents and ensure their hard drive or flash memory is

erased, encrypted or destroyed prior to being returned to the leasing company, sold to a third party or otherwise disposed of. (Per FIL 56-2010).


FIL 56-2010

Examiner Comments:

If needed, provide additional comments regarding the bank's operation security and risk management function.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

11- INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 3 – AUDIT/INDEPENDENT REVIEW PROGRAM

Assess how the institution monitors operations and compliance with a written information security program.

1. Evaluate and comment upon the degree to which the risk analysis process ensures that audit plans address all significant IT operations, procurement, and development activities with appropriate scope and frequency.

Examiner Comments:

2. Evaluate and comment upon the degree to which the audit function is independent and identifies and reports weaknesses and risks to the Board of Directors or its audit committee in a thorough and timely manner.

Examiner Comments:

3. Evaluate and comment upon whether outstanding audit issues are monitored until resolved.

Examiner Comments:

4. Evaluate and comment upon whether audit work is performed in accordance with professional auditing standards and report content is timely, constructive, accurate, and complete.

Examiner Comments:

5. Evaluate and comment upon the degree to which the board of directors and examiners can rely on the audit results.

Examiner Comments:

If needed, provide additional comments regarding the bank's audit and independent review function.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

11- INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 4 - DISASTER RECOVERY AND BUSINESS CONTINUITY

Assess the institution's level of preparedness for responding to and recovering from an unexpected event.

1. Evaluate and comment upon whether management has a comprehensive corporate contingency and business resumption program in place.

Examiner Comments:

2. Evaluate and comment upon whether annual contingency plan testing and updating is adequate, and whether test results evidence that critical systems and applications are recovered within acceptable time frames.

Examiner Comments:

If needed, provide additional comments regarding the bank's disaster recovery and business continuity management function.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

11- INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 5 – Vendor Management and Service Provider Oversight

Given the increased reliance on outside firms for technology-related products and services, assess the effectiveness of the vendor management and service provider oversight programs.

1. Evaluate and comment upon the degree to which outsourcing arrangements are based on comprehensive planning, and whether routine management supervision sustains an appropriate level of control over vendor contracts, performance, and services provided.

Examiner Comments:

If needed, provide additional comments regarding the bank's vendor management program.

Additional Comments:

Institution		**Date of Exam**	
Charter		**Prepared By**	

11- INFORMATION TECHNOLOGY SNAPSHOT WORKPROGRAM

PART 6 – INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

Evaluate if the bank's information security program adequately meets the objectives of safeguarding customer information guidelines and subsequent interpretive guidance.

- Ensures the security and confidentiality of customer information;
- Protects against any anticipated threats or hazards to the security or integrity of such information;
- Protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer;
- Ensures the proper disposal of customer information and consumer information.
- Implements appropriate authentication in an Internet banking environment; and
- Ensures appropriate response programs for unauthorized access.

Examiner Comments:

Complete the Summary of Findings.

SUMMARY OF FINDINGS

#11 – IT RMP

Describe all strengths evident from the evaluation.

Describe all weaknesses evident from evaluation, including violations of law/regulation/rules; noncompliance with Departmental policies/guidelines; internal policy deficiencies/ noncompliance; internal control weaknesses; MIS problems; and deficiencies in management supervision.

Report Worthy:

Not Report Worthy:

Determine why weaknesses exist and comment on management's response and plan of action. Identify bank personnel making the response.

SUMMARY RISK RATING ASSIGNED: ☐

Definitions:

1-Strong; 2-Satisfactory; 3-Less than satisfactory; 4-Deficient; 5-Critically deficient; NR-Not Rated

➤ **(Return to Core Analysis)**

Provide copy of this page to EIC/AEIC. Receipt and review of this form by the EIC/AEIC will be evidenced bsy his/her initials in the appropriate column for this procedure on the SCOPE AND WAIVER FORM.